

FILED
LODGED

AO 106 (Rev. 04/10) Application for Search Warrant

JUN -1 2016

UNITED STATES DISTRICT COURT

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY
BY

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Microsoft/Skype account with username "kjomart1"

Case No.

MT16-252

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Microsoft/Skype account with username "kjomart1" further described in Attachment A, attached hereto,
located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

SEE Attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

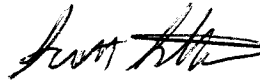
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2);	Receipt or Distribution of Depictions of Minors Engaged in Sexually Explicit Conduct;
18 U.S.C. § 2252(a)(4)(B)	Possession of Depictions of Minors Engaged in Sexually Explicit Conduct

The application is based on these facts:

SEE Affidavit of S/A Scott Sutehall.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SCOTT SUTEHALL, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

6/1/16



Judge's signature

City and state: Seattle, Washington

BRIAN A. TUSCHIDA, United States Magistrate Judge

Printed name and title

2016R00446

ATTACHMENT A

Place to Be Searched

The electronically stored information and communications contained in, and associated with Skype username "kjomart1," as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Microsoft Corporation, headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

ITEMS TO BE SEIZED

Section I – Items to be provided by Microsoft/Skype for Search

All electronically stored information and communications contained in the Skype account/username “kjomart1” for the past 180 days, including, but not limited to:

- a. Information captured at the time of account registration, including the date and time of account opening, the user’s full name, billing address, date of birth, phone number, related email account(s), alias(es), screen name(s), and the IP address from which the account was created;
- b. The user’s payment method, including checking and/or credit card number(s), and detailed billing records;
- c. Skype Numbers currently subscribed to, as well as a historical list of Skype Number(s) subscribed to;
- d. Historical call detail records for calls placed to the public switched telephone network (PSTN);
- e. Historical call detail records for calls received from the public switched telephone network (PSTN);
- f. SMS historical detail records;
- g. Historical Skype WiFi hotspots records;
- h. Historical record of e-mail and password change activity;
- i. The user’s Skype contact/buddy list;
- j. Any and all other log records, including IP address captures;
- k. The user’s chat records and media content, including the content of all messages sent and received for the past 180 days, the date and time those messages were sent, the type of Skype client/application (website, desktop, mobile, etc.) used to send/receive the message, the Skype username(s) of the message sender and receiver, and all media, including but not limited to images, videos, and/or audio recordings, sent and received.

ATTACHMENT B

ITEMS TO BE SEIZED

Section II – Items to be Seized

From all electronically stored information and communications contained in the Microsoft/Skype account/username “kjomart1”:

- a. All messages, attachments, documents, and profile information, or other data that serves to identify any persons who use or access the account specified, or who exercise, in any way, any dominion or control over the specified account;
- b. Any address lists or buddy/contact lists associated with the specified account;
- c. All images and/or videos depicting child pornography, any messages or documents relating to the transmission of child pornography (including any attachments thereto), any evidence of child sexual abuse, and any other data that otherwise constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Depictions of Minors Engaged in Sexually Explicit Conduct) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Depictions of Minors Engaged in Sexually Explicit Conduct);
- d. All subscriber records associated with the specified account, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account numbers;
- e. Any and all other log records, including IP address captures, associated with the specified account; and
- f. Any records of communications between Microsoft/Skype, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider’s support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

1 **AFFIDAVIT**

2 STATE OF WASHINGTON)
 3) ss
 4 COUNTY OF KING)

5 **I. INTRODUCTION**

6 I, Scott Sutehall, being first duly sworn on oath, depose and say:

7 1. I am a Special Agent (SA) with the U.S. Department of Homeland Security,
 8 Homeland Security Investigations (HSI), assigned to the Seattle, Washington, field office.
 9 HSI is responsible for enforcing the customs and immigration laws and federal criminal
 10 statutes of the United States. I have been an agent with HSI since 2008, assigned to the
 11 Child Exploitation Unit since 2013. As part of my duties I investigate criminal violations
 12 relating to child exploitation and child pornography, including violations pertaining to the
 13 illegal production, distribution, receipt, and possession of child pornography and material
 14 involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and
 15 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI
 16 Special Agent Training Program, and have received further specialized training in
 17 investigating child pornography and child exploitation crimes. I have also had the
 18 opportunity to observe and review examples of child pornography (as defined in 18 U.S.C.
 19 § 2256(8)). I have participated in the execution of previous search warrants which involved
 20 child exploitation and/or child pornography offenses and the search and seizure of computers
 21 and other digital devices. I am a member of the Seattle Internet Crimes Against Children
 22 (ICAC) Task Force in the Western District of Washington, and work with other federal,
 23 state, and local law enforcement personnel in the investigation and prosecution of crimes
 24 involving the sexual exploitation of children.

25 2. I make this Affidavit in support of an application for a search warrant, pursuant
 26 to 18 U.S.C. § 2703, to search the electronic communications contained in the
 27 Microsoft/Skype account with username "kjomart1" (hereinafter the SUBJECT SKYPE
 28 ACCOUNT) more fully described in Attachment A to this Affidavit, attached hereto and

1 incorporated herein, as well as all other subscriber and log records associated with this
2 account, to seize the items listed in Attachment B, attached to this Affidavit and incorporated
3 herein by reference, for evidence, fruits, and instrumentalities of violations of 18 U.S.C.
4 § 2252(a)(2) (Receipt or Distribution of Depictions of Minors Engaged in Sexually Explicit
5 Conduct), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Depictions of Minors Engaged in
6 Sexually Explicit Conduct).

7 3. The facts set forth in this Affidavit are based on my own personal knowledge;
8 knowledge obtained from other individuals during my participation in this investigation,
9 including other law enforcement officers; review of documents and records related to this
10 investigation; communications with others who have personal knowledge of the events and
11 circumstances described herein; and information gained through my training and experience.

12 4. Because this Affidavit is submitted for the limited purpose of establishing
13 probable cause in support of the application for a search warrant, it does not set forth each
14 and every fact that I or others have learned during the course of this investigation. I have set
15 forth only the facts that I believe are relevant to the determination of probable cause to
16 believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2)
17 (Receipt or Distribution of Depictions of Minors Engaged in Sexually Explicit Conduct) and
18 18 U.S.C. § 2252(a)(4)(B) (Possession of Depictions of Minors Engaged in Sexually Explicit
19 Conduct), will be found in the SUBJECT SKYPE ACCOUNT.

20 II. STATEMENT OF PROBABLE CAUSE

21 Case Initiation: Investigation of Jeffrey Gibson

22 5. In January 2016, while acting in an undercover capacity, I utilized a law
23 enforcement version of eMule, a commonly used peer-to-peer (P2P) file sharing program for
24 the eD2k file sharing network, to monitor for P2P users possessing and distributing image
25 and video files depicting child pornography. I utilized the law enforcement version of eMule
26 to download several files depicting child pornography from a P2P user at IP address
27 67.160.23.81.
28

1 6. A query of a publicly available database revealed IP address 67.160.23.81
2 belonged to Internet Service Provider (ISP) Comcast Communications.

3 7. In January 2016, I submitted two Department of Homeland Security (DHS)
4 administrative summonses to Comcast requesting subscriber information for IP address
5 67.160.23.81 during the dates and times the subject video files were downloaded. Comcast
6 provided the requested information: on the dates and times the subject video files were
7 downloaded, IP address 67.160.23.81 was assigned to Jeffrey Gibson (hereinafter "Gibson")
8 at the residence located at a residence on 222nd Street SW, Mountlake Terrace, Washington
9 (hereinafter the "Mountlake Terrace residence").

10 8. The investigation revealed that Gibson resided at the Mountlake Terrace
11 residence with his girlfriend (hereinafter "Girlfriend"), his minor daughter (hereinafter
12 "Daughter"), and girlfriend's mother, (hereinafter "Mother").

13 9. On February 8, 2016, I obtained a federal search warrant for the Mountlake
14 Terrace residence. On February 12, 2016, HSI agents, including myself, executed the
15 warrant at the Mountlake Terrace residence. Agents encountered Gibson, Girlfriend,
16 Mother, and Daughter living at the residence.

17 10. U.S. Postal Inspector Samantha Knoll and I attempted to interview Gibson in a
18 law enforcement vehicle parked in front of the residence. After I showed Gibson a copy of
19 the search warrant and read Gibson his Miranda rights, he stated that he wanted an attorney
20 present before answering any questions. No questions were asked.

21 11. During the search of the Mountlake Terrace residence, several computers and
22 digital devices were forensically examined (onsite) by HSI Computer Forensic Agents.
23 During the onsite examination of an Asus laptop, which was found on the floor in Gibson
24 and Girlfriend's bedroom, on Gibson's side of the bed, agents located child pornography
25 files. During the warrant service, I showed Girlfriend this Asus laptop and asked who owned
26 and used the device. Girlfriend told me that it belonged to Gibson and was exclusively used
27 by Gibson. In addition this Asus laptop, several other computers, digital devices, and digital
28 media were seized from the residence pursuant to the search warrant.

1 12. At the conclusion of the warrant service, Gibson was arrested by Snohomish
2 County Sheriff's Office Detective Nicole Richardson based on probable cause that he
3 committed the following violation of Washington State law: RCW 9.68A.050, Dealing
4 Depictions of Minors Engaged in Sexually Explicit Conduct, and RCW 9.68A.070,
5 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct. On or about
6 March 2, 2016, Gibson was released and is not currently in custody.

7 13. The digital devices seized from the Mountlake Terrace residence were
8 examined and searched by HSI Computer Forensic Agents at the HSI Seattle office. The
9 examination revealed Gibson possessed thousands of child pornography image and video
10 files on several of the seized devices. Those devices included the aforementioned Asus
11 laptop computer, a Sony laptop computer, a Toshiba laptop computer, a Samsung cell phone,
12 a 32 gigabyte (GB) USB thumb drive, and four CDs/DVDs. On the Asus laptop,
13 approximately 4,000 child pornography files were located, including several video files
14 depicting the sexual abuse of babies and toddlers. The examination also revealed that the
15 eMule P2P software program was installed on the Asus laptop. Furthermore, the user hash
16 ID – which is a unique identifying number assigned to each specific software program
17 installed on a computer – of the eMule program installed on the Asus laptop exactly matched
18 the user hash ID of the eMule program used by the P2P user from which I covertly
19 downloaded child pornography files to initiate the investigation.

20 **Information obtained from Gibson during proffer**

21 14. On or about March 28, 2016, Gibson's attorney (hereinafter "Defense
22 Attorney"), informed Robert Grant, Deputy Prosecuting Attorney with the Snohomish
23 County Prosecutor's Office, that Gibson may have information about an individual allegedly
24 involved in producing child pornography.

25 15. On May 3, 2016, at approximately 2:30 p.m., a proffer was conducted with
26 Gibson at the Snohomish County Prosecutor's Office. SA Adam Anderson, Deputy
27 Prosecuting Attorney Robert Grant, Gibson, Defense Attorney, and I were present. A proffer
28 agreement between the State of Washington and Gibson was signed by Gibson and Defense

1 Attorney at the outset of the proffer. During the ensuing proffer, Gibson stated the
2 following, non-verbatim:

3 16. On or about the summer of 2015, Gibson responded to an advertisement (ad)
4 on Craigslist.com. Gibson was unsure exactly what the ad stated, but said it related to
5 "taboo" sexual interests. Gibson communicated with the individual who posted the ad via
6 his Hotmail email account. Soon thereafter, Gibson met this individual in person near the
7 Northgate Mall in Seattle, Washington, for approximately thirty minutes. During the
8 meeting they discussed their sexual and/or taboo interests. Gibson said the individual's
9 name is KYLE TATE. Gibson stated that KYLE TATE was Filipino, but was unsure where
10 KYLE TATE was born. Gibson stated KYLE TATE was gay, and believed he is
11 approximately thirty years old.

12 17. Gibson met with KYLE TATE on one other occasion, at KYLE TATE's
13 residence in Seattle. Gibson could not recall the address, but said he could identify where
14 this residence was located if shown a map. Mr. Grant proceeded to show Gibson a map (on
15 his cell phone). Gibson navigated the map and pointed to the intersection of Stone Avenue
16 North and North 49th Street, stating that KYLE TATE's residence was one of the first two or
17 three houses west of Stone Avenue North, on the south side of North 49th Street. When
18 asked what KYLE TATE's residence looked like, Gibson stated there were stairs that
19 worked from right to left (when facing the residence from North 49th Street) from the
20 sidewalk up to the front porch of the residence. Gibson was unsure of the color, but said the
21 house might have been blue.

22 18. During the meeting at KYLE TATE's residence, which also lasted
23 approximately thirty minutes, Gibson stated that he and KYLE TATE viewed and exchanged
24 electronic files depicting child pornography. Gibson stated KYLE TATE possessed child
25 pornography files on his (KYLE TATE's) Apple MacBook laptop and cell phone. Gibson
26 could not recall what brand of cell phone KYLE TATE had, but said it was not an Apple
27 product. Gibson further stated that KYLE TATE physically showed him (Gibson) child
28 pornography files on both of those devices. When asked what kind of child pornography

1 files KYLE TATE possessed and showed him, Gibson said the child pornography files
2 depicted very young children, and mostly boys.

3 19. Gibson stated that he believed KYLE TATE worked for a childcare facility or
4 at a school, but was unsure of the name or location of the facility.

5 20. Gibson stated KYLE TATE said that he had a niece, approximately four years
6 old, whom he often watched or babysat. Gibson stated KYLE TATE said he would "play"
7 with his niece when he babysat her. Gibson stated that KYLE TATE never actually told him
8 that he sexually abused his niece, but Gibson believed KYLE TATE may have meant he was
9 sexually abusing his niece by the way he said he "played" with her. Gibson said that KYLE
10 TATE emailed Gibson on at least one occasion stating that he was watching his niece and
11 invited Gibson over to KYLE TATE's residence. Gibson stated he never met KYLE
12 TATE's alleged niece, and that he believed the above described meeting at KYLE TATE's
13 residence was the last time they met in person.

14 21. When asked if he knew how KYLE TATE obtained child pornography files,
15 Gibson stated that, in addition to meeting with child pornography collectors in person, he
16 recalled KYLE TATE told him he used Skype. Gibson didn't believe KYLE TATE used
17 P2P file sharing networks to obtain or share child pornography. Gibson stated he and KYLE
18 TATE only exchanged child pornography files in person, and that they didn't use email or
19 any other electronic methods. Gibson recalled that KYLE TATE did have a Facebook
20 profile.

21 **Investigation of KYLE TATE**

22 22. Records checks conducted via law enforcement databases revealed that KYLE
23 TATE (DOB 1982; SSN XXX-XX-6600) has been associated with the residence located at
24 1223 North 49th Street, Seattle, Washington (hereinafter the "SUBJECT PREMISES") since
25 approximately July 2014. Records checks conducted via the Washington State Department
26 of Licensing (WSDOL) revealed that on March 5, 2016, KYLE TATE was issued a driver's
27 license in which the address listed is the SUBJECT PREMISES.
28

1 23. On May 5, 2016, an official with the United States Postal Inspection service
2 told me that individuals with the last name Tate and an individual referred hereafter as
3 "INDIVIDUAL Y" are receiving mail at the SUBJECT PREMISES.

4 24. Open source research conducted on KYLE TATE's Facebook page revealed
5 that KYLE TATE attended Whitworth University (in Spokane, Washington) and grew up in
6 Basin, Wyoming. Further, because KYLE TATE's Facebook page is open and viewable by
7 anyone, I was able to view several albums that contained dozens of photos of KYLE TATE,
8 in various settings. The photos of KYLE TATE on his Facebook page match the photo of
9 KYLE TATE on his Washington State driver's license.

10 25. Also while reviewing KYLE TATE's Facebook account, I observed that on
11 January 30, 2014, KYLE TATE made a post to his Facebook page, stating: "My very first
12 Mac! My partner, a former Microsoft employee, wasn't happy.....Oh well! It's really pretty."
13 A picture was attached to this post that depicted a silver Apple MacBook Air laptop
14 computer. The laptop is resting on a white MacBook Air box, which appears to be on a table
15 or desk. Thus, it appears KYLE TATE purchased an Apple MacBook Air laptop on or
16 before January 30, 2014. As stated above, during the aforementioned proffer, Gibson stated
17 that during the summer of 2015 he viewed child pornography files on KYLE TATE's Apple
18 MacBook laptop computer.

19 26. On May 4, 2016, I submitted a DHS Summons to Comcast requesting
20 subscriber information and IP address connection history for the SUBJECT PREMISES.
21 Later on May 4, 2016, Comcast responded, stating that INDIVIDUAL Y is the current
22 subscriber of internet service at the SUBJECT PREMISES.

23 27. Records checks conducted via the King County Assessor's Office revealed that
24 the SUBJECT PREMISES, a single family residence built in 1918, contains approximately
25 820 square feet (finished) and 360 square feet (unfinished), and is owned by a person
26 hereinafter referred to as "INDIVIDUAL P."

27 28. Additional records checks conducted via the WSDOL revealed that on
28 March 21, 2014, INDIVIDUAL Y (DOB 1963) was issued a driver's license in which the

1 address listed was the SUBJECT PREMISES. Additionally, on May 29, 2015, another
2 person (hereinafter referred to as "INDIVIDUAL O" (DOB 1965)), was issued a driver's
3 license in which the address listed was the SUBJECT PREMISES.

4 29. On May 4, 2016, I conducted surveillance of the SUBJECT PREMISES. I
5 observed that the SUBJECT PREMISES is located at the intersection of Stone Avenue North
6 and North 49th St. I also observed that the SUBJECT PREMISES is located on the south
7 side of North 49th Street, and is the first house west of Stone Avenue North. When facing
8 the SUBJECT PREMISES, stairs lead up from the sidewalk to an elevated front porch, from
9 right to left. This information matches very closely the information provided by Gibson
10 during the proffer detailed above. However, I observed the SUBJECT PREMISES to have
11 white colored wood siding, while Gibson thought the color of KYLE TATE's house might
12 be blue (stated above).

13 30. While conducting surveillance of the SUBJECT PREMISES I observed a
14 white Chevy Malibu sedan parked on the street directly in front of the SUBJECT
15 PREMISES. Records checks revealed that this vehicle is registered to KYLE TATE at the
16 SUBJECT PREMISES. The registration expires on August 1, 2016. I also observed a green
17 Subaru parked on the street in front of the SUBJECT PREMISES, which is registered to
18 INDIVIDUAL Y at the SUBJECT PREMISES. I did not observe any vehicles in the vicinity
19 registered to INDIVIDUAL O.

20 31. At approximately 8:00 a.m. I observed a white male exit the SUBJECT
21 PREMISES through the front door and depart the area in a white Toyota pickup truck with
22 "Food Bank" markings on the truck. Records checks revealed this vehicle is registered to the
23 University District Food Bank at 4731 15th Avenue North, Seattle, WA 98105. I believe the
24 individual who departed in the Toyota truck may have been INDIVIDUAL Y, based on a
25 photo I have seen of INDIVIDUAL Y.

26 32. At approximately 8:25 a.m. I observed an individual who I believed to be
27 KYLE TATE (based on several photos I had seen of KYLE TATE) exit the SUBJECT
28 PREMISES through the front door and depart the area on foot. I followed KYLE TATE

1 several blocks on foot and observed KYLE TATE board a King County Metro bus, route 62.
2 I boarded the bus and sat a few seats behind KYLE TATE. I observed that on several
3 occasions KYLE TATE used a white Samsung cell phone. At approximately 8:55 a.m. I
4 observed KYLE TATE get off the bus at the intersection of Dexter Avenue North and Aloha
5 Street. I followed KYLE TATE on foot for several blocks and observed KYLE TATE walk
6 into a building at 1210 Valley Street, Seattle, WA 98109 at approximately 9:05 a.m. I
7 observed that there was an outdoor playground adjacent to the side door of the building. I
8 also noticed that KYLE TATE entered the building through the playground and side door,
9 rather than the front door.

10 33. Later on May 4, 2016, I conducted open source Internet research of the
11 business located at 1210 Valley Street and learned that it is the Hutch Kids Child Care
12 Center, a child care center for employees of the Fred Hutchinson Cancer Research Center
13 that enrolls and cares for infants, toddlers, and preschool-aged children. On the website for
14 the Hutch Kids Child Care Center, I located a section called Staff Biographies. Under
15 "Teaching Staff" I observed a list of biographical narratives for several individuals, listed by
16 first name. I observed the following narrative under the name "Kyle:"

17 "I grew up in Basin, Wyoming, and attended Whitworth College (it changed its
18 name to Whitworth University after I graduated) in Spokane, WA, where I
19 graduated with a Bachelor of Arts in Music. I have worked as a tutor in high
20 school for elementary students and as an ESL tutor during my college
21 education for Spokane Public Schools. After graduation of college I worked as
22 a caregiver for adults with developmental disabilities, as well as for the elderly.
23 Before coming to Hutch Kids I worked for the YMCA in their childhood
24 program, and as a preschool teacher for a corporate child care center. I also
25 have taught individual music lessons to both adults and children in my spare
26 time. I enjoy running half and full marathons, cycling, playing volleyball and
27 ultimate Frisbee."

28 34. The information provided in this biography – namely growing up in Basin,
Wyoming, and attending Whitworth College – matches information found on KYLE TATE's
Facebook page. It appears that in addition to currently working as a child care provider at a

1 local child care facility, KYLE TATE has tutored elementary school aged children, taught
2 music lessons to children, and worked as a childcare provider at multiple businesses and/or
3 facilities in the past.

4 35. On May 5, 2016, HSI Computer Forensic Agents conducted additional
5 examination of the devices seized from Gibson on February 12, 2016. On Gibson's seized
6 Samsung cell phone, which was found on the floor in Gibson and Girlfriend's bedroom, on
7 Gibson's side of the bed, Computer Forensic Agent (CFA) Natane Adkins located a contact
8 under the name "Kyle" with phone number 206-861-2168. This phone number is an exact
9 match of a cell phone number listed for KYLE TATE in a law enforcement database.

10 36. On May 5, 2016, I obtained a federal search warrant for the SUBJECT
11 PREMISES from United States Magistrate Judge Mary Alice Theiler. On May 6, 2016, I,
12 along with other law enforcement officers, executed the warrant at the SUBJECT
13 PREMISES.

14 37. At approximately 8:15 a.m., Seattle Police Department (SPD) Detective Daljit
15 Gill and I interviewed KYLE TATE inside a law enforcement vehicle parked in front of the
16 SUBJECT PREMISES. I showed KYLE TATE a copy of the search warrant, including
17 attachments, which he read. I stated that agents would be searching his residence for
18 evidence of child pornography. KYLE TATE said he understood. At approximately
19 8:18 a.m. I read KYLE TATE his Miranda rights. He stated that he understood his rights and
20 that he would answer questions and talk with us about the investigation. During the
21 interview, KYLE TATE admitted to possessing child pornography files, both videos and
22 images, on a white and black thumb drive that was located in his residence. He said there
23 would be hundreds, if not thousands, of child pornography files on this thumb drive. KYLE
24 TATE physically showed me and other agents where the USB thumb drive was located,
25 which was inside a zippered pocket of a backpack inside the SUBJECT PREMISES. He said
26 he would plug this USB thumb drive into his Apple MacBook Air laptop computer to view
27 the child pornography files. He said he most recently viewed the child pornography files
28 about two weeks prior. He said he would sometimes masturbate while viewing the child

1 pornography files. During the onsite examination of the USB thumb drive (a 64GB PNY
2 drive) by HSI Computer Forensic Agents, agents located child pornography files.

3 38. KYLE TATE said he obtained the child pornography files when he met with
4 two individual he met over Craigslist. He explained that he met both individuals in person at
5 his residence, the SUBJECT PREMISES, within the last two years. He said the other
6 individuals gave him USB thumb drives containing child pornography, including the white
7 and black USB thumb drive described above.

8 39. KYLE TATE said he conducts video chats/calls via Skype during which he
9 views images and videos depicting child pornography with others. KYLE TATE further
10 stated that he has masturbated while viewing child pornography files over Skype video chats.
11 KYLE TATE said his Skype username is "kjomart1" (the SUBJECT SKYPE ACCOUNT).

12 40. KYLE TATE confirmed that he works for the Hutch Kids Child Care Center.
13 He said he works as an "infant teacher." He said he's worked for this child care facility for
14 approximately five years. Prior to that, he worked for the Kindercare childcare center near
15 Northgate Mall in Seattle for approximately two years, primarily with two and three year
16 olds. Prior to that, he worked for the YMCA attached to the T.T. Minor Elementary in
17 Seattle, in their before/after school daycare program.

18 41. KYLE TATE stated that he has had fantasies about sexually abusing children,
19 boys and girls, ranging from infants to middle school ages. He fantasized about "helping
20 them explore a man's body." He fantasized about children touching him on his genitals and
21 about him touching them on their genitals. He also fantasized about inserting his penis into a
22 child's mouth and anus.

23 42. KYLE TATE stated that during video chat conversations over Skype, he
24 discussed trying to find a child to help them "explore his body." He also talked to people
25 over Skype video calls about going to another country, possibly Thailand or somewhere in
26 Asia or Europe, to find children to "play with," "be naked with," and "be sexual with." He
27 said he talked about doing this with elementary or middle school-aged children.
28

1 43. KYLE TATE admitted to having urges to inappropriately touch or molest
2 children and that he recently acted on those urges. He said he had urges to touch a female
3 infant he recently babysat. He said he currently takes care of this infant at the Hutch Kids
4 Child Care Center, and that he babysat the infant on the side at the family's home in or about
5 October 2015. He said the infant is eleven months old. He said he fantasized about "what it
6 would feel like to put his finger inside her vagina." He said that while he was changing the
7 infant's diaper on a changing table, after he used wet wipes to clean her and put diaper cream
8 on her, he "grazed his finger over her anus." When asked what he was thinking at the time,
9 he said he didn't know what he was thinking, but stated he "had an urge."

10 44. At the conclusion of the warrant service, KYLE TATE was arrested based on
11 probable cause that he committed violations of 18 U.S.C. § 2252(a)(4)(B) (Possession of
12 Depictions of Minors Engaged in Sexually Explicit Conduct).

13 45. The digital devices seized from the SUBJECT PREMISES examined and
14 searched by HSI Computer Forensic Agents at the HSI Seattle office pursuant to the search
15 warrant. The examination revealed KYLE TATE possessed thousands of child pornography
16 image and video files – including dozens of files depicting the sexual abuse of babies and
17 toddlers – on several of the seized devices. Child pornography files were located on the
18 aforementioned white and black PNY 64GB USB flash drive, a Blackberry cell phone, and a
19 Dell laptop computer.

20 46. Additionally, agents located evidence of Skype chat logs on KYLE TATE's
21 seized Apple MacBook Air laptop and Blackberry cell phone. The Skype username on both
22 of those devices is "kjomart1" (the SUBJECT SKYPE ACCOUNT). As stated above,
23 during the interview of KYLE TATE on May 6, 2016, he said his Skype username was
24 "kjomart1" (the SUBJECT SKYPE ACCOUNT).

25 47. In summary, during a proffer with Gibson on May 3, 2016, he recalled that
26 KYLE TATE told him that he (KYLE TATE) obtained child pornography files via Skype.
27 During the interview of KYLE TATE on May 6, 2016, he stated that he viewed child
28 pornography files over Skype video chats and that he masturbated during those video chat

1 sessions. KYLE TATE also said he conversed with others over Skype video chats about
2 sexually abusing children and possibly travelling to other countries to sexually abuse
3 children. KYLE TATE told me that his Skype username was "kjomart1" (the SUBJECT
4 SKYPE ACCOUNT). During the examination and search of digital devices seized from
5 KYLE TATE, agents located this exact Skype account/username on multiple devices, as well
6 as a large collection of child pornography files.

7 **III. PAST EFFORTS TO OBTAIN EVIDENCE**

8 48. I understand that certain contents of the SUBJECT SKYPE ACCOUNT
9 (identified in Paragraph 2) can only be obtained, in the Ninth Circuit, by means of a search
10 warrant issued under authority of 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and
11 Federal Rule of Criminal Procedure 41(e)(2)(b). To my knowledge, there have been no prior
12 attempts to secure a search warrant to search and seize these records. However, on May 12,
13 2016, I submitted a Preservation Request to Microsoft Corporation requesting that records
14 and evidence relating to the SUBJECT SKYPE ACCOUNT be preserved pursuant to
15 18 U.S.C. §§ 2703(f), pending further legal process. On May 23, 2016, the Preservation
16 Request was confirmed and assigned reference number 255667.

17 **IV. GENUINE RISKS OF DESTRUCTION OF EVIDENCE**

18 49. Based upon my experience and training, it is not uncommon for technically
19 sophisticated criminals to use encryption or programs to destroy data that can be triggered
20 remotely, or by a pre-programed event or keystroke, or other sophisticated techniques to hide
21 data. In this case, the data this application seeks is stored on an enterprise storage system,
22 also known as a server, belonging to Microsoft/Skype. If that data is accessed and deleted by
23 the user, by either deleting the emails or any associated contact lists, the content would not
24 be retrievable. Unlike traditional computer forensics where a hard drive can be searched and
25 deleted documents recovered, information stored in an enterprise storage system is
26 irretrievable once it has been deleted. Further, since this information is accessible from
27 anywhere that the suspect can obtain an Internet connection to log on to his account, he can
28 delete this information in a matter of minutes.

V. PROTOCOL FOR SORTING SEIZABLE ELECTRONICALLY STORED INFORMATION

50. In order to ensure that agents are limited in their search only to the SUBJECT SKYPE ACCOUNT (and any attachments, stored messages, stored voice messages, documents, and photographs/videos associated therewith); in order to protect the privacy interests of other third parties who have accounts at Microsoft/Skype; and in order to minimize disruptions to normal business operations of Microsoft/Skype; this application seeks authorization to permit agents and employees of Microsoft/Skype to assist in the execution of the warrant, pursuant to 18 U.S.C. § 2703(g) as follows:

- a. The search warrant will be presented to Microsoft/Skype, with direction that it identify and isolate associated records described in Section I of Attachment B.
- b. Microsoft/Skype will also be directed to create an exact duplicate in electronic form of the email account and records specified in Section I of Attachment B, including an exact duplicate of the content of all messages stored in the specified account.
- c. Microsoft/Skype shall then provide an exact digital copy of the contents of the SUBJECT SKYPE ACCOUNT, as well as all other records associated with the account, to me or to any other agent of HSI. Once the digital copy has been received from Microsoft/Skype, that copy will, in turn, be forensically imaged and only that image will be reviewed and analyzed to identify communications and other data subject to seizure pursuant to Section II of Attachment B. The original digital copy will be sealed and maintained to establish authenticity, if necessary.
- d. I and/or other agents of HSI will thereafter review the forensic image, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure. I and/or other agents of HSI will then copy those items identified for seizure to separate media for future use in the investigation and prosecution. The forensic copy of the

1 complete content of the email accounts will also then be sealed and retained by
2 HSI, and will not be unsealed absent Court authorization, except for the
3 purpose of duplication of the entire image in order to provide it, as discovery,
4 to a charged defendant.

5 e. Analyzing the data contained in the forensic image may require special
6 technical skills, equipment, and software. It could also be very time-
7 consuming. Searching by keywords, for example, can yield thousands of
8 "hits," each of which must then be reviewed in context by the examiner to
9 determine whether the data is within the scope of the warrant. Merely finding
10 a relevant "hit" does not end the review process. Keywords used originally
11 need to be modified continuously, based on interim results. Certain file
12 formats, moreover, do not lend themselves to keyword searches, as keywords
13 search text, and many common electronic mail messaging, database, and
14 spreadsheet applications do not store data as searchable text. The data is
15 saved, instead, in proprietary non-text format. And, as the volume of storage
16 allotted by service providers increases, the time it takes to properly analyze
17 recovered data increases, as well. Consistent with the foregoing, searching the
18 recovered data for the information subject to seizure pursuant to this warrant
19 may require a range of data analysis techniques and may take weeks or even
20 months.

21 f. Based upon my experience and training, and the experience and training of
22 other agents with whom I have communicated, it is necessary to seize all
23 messages, chat logs, and documents, that identify any users of the subject
24 account and any messages sent or received in temporal proximity to
25 incriminating messages that provide context to the incriminating
26 communications.

1 g. All forensic analysis of the image data will employ only those search protocols
2 and methodologies reasonably designed to identify and seize the items
3 identified in Section II of Attachment B to the warrant.

4 **VII. CONCLUSION**

5
6 51. Based upon the evidence gathered in this investigation and set out above,
7 including, but not limited to, my review of data and records, information received from other
8 law enforcement agents, and my training and experience, there is probable cause to believe
9 that evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt
10 or Distribution of Depictions of Minors Engaged in Sexually Explicit Conduct), and
11 18 U.S.C. § 2252(a)(4)(B) (Possession of Depictions of Minors Engaged in Sexually Explicit
12 Conduct) exists and will be found in the electronically stored information or communications
13 contained and associated with the SUBJECT SKYPE ACCOUNT (Microsoft/Skype account
14 with username "kjomart1") (and any attachments, multimedia messages, stored instant
15 messages, stored voice messages, documents, and images/videos associated therewith), as
16 well as in subscriber and log records associated with this account.

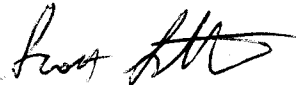
17 ///

18 ///

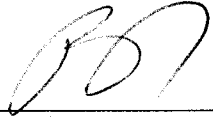
19 ///

1 53. Accordingly, by this Affidavit and warrant I seek authority for the government
2 to search all of the items specified in Section I, Attachment B (attached hereto and
3 incorporated by reference herein) to the warrant, and specifically to seize all of the data,
4 documents and records that are identified in Section II to that same Attachment.

5 DATED this _____ day of _____, 2016.

6
7 
8 _____
9 SCOTT SUTEHALL, AFFIANT
10 Special Agent
11 Department of Homeland Security
12 Homeland Security Investigations

13 SUBSCRIBED and SWORN to before me this 1st day of June,
14 2016.

15 
16 _____
17 BRIAN A. TSUCHIDA
18 United States Magistrate Judge
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A

Place to Be Searched

The electronically stored information and communications contained in, and associated with Skype username "kjomart1," as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Microsoft Corporation, headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

ITEMS TO BE SEIZED

Section I – Items to be provided by Microsoft/Skype for Search

All electronically stored information and communications contained in the Skype account/username “kjomart1” for the past 180 days, including, but not limited to:

- a. Information captured at the time of account registration, including the date and time of account opening, the user’s full name, billing address, date of birth, phone number, related email account(s), alias(es), screen name(s), and the IP address from which the account was created;
- b. The user’s payment method, including checking and/or credit card number(s), and detailed billing records;
- c. Skype Numbers currently subscribed to, as well as a historical list of Skype Number(s) subscribed to;
- d. Historical call detail records for calls placed to the public switched telephone network (PSTN);
- e. Historical call detail records for calls received from the public switched telephone network (PSTN);
- f. SMS historical detail records;
- g. Historical Skype WiFi hotspots records;
- h. Historical record of e-mail and password change activity;
- i. The user’s Skype contact/buddy list;
- j. Any and all other log records, including IP address captures;
- k. The user’s chat records and media content, including the content of all messages sent and received for the past 180 days, the date and time those messages were sent, the type of Skype client/application (website, desktop, mobile, etc.) used to send/receive the message, the Skype username(s) of the message sender and receiver, and all media, including but not limited to images, videos, and/or audio recordings, sent and received.

ATTACHMENT B

ITEMS TO BE SEIZED

Section II – Items to be Seized

From all electronically stored information and communications contained in the Microsoft/Skype account/username “kjomart1”:

- a. All messages, attachments, documents, and profile information, or other data that serves to identify any persons who use or access the account specified, or who exercise, in any way, any dominion or control over the specified account;
- b. Any address lists or buddy/contact lists associated with the specified account;
- c. All images and/or videos depicting child pornography, any messages or documents relating to the transmission of child pornography (including any attachments thereto), any evidence of child sexual abuse,, and any other data that otherwise constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Depictions of Minors Engaged in Sexually Explicit Conduct) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Depictions of Minors Engaged in Sexually Explicit Conduct);
- d. All subscriber records associated with the specified account, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account numbers;
- e. Any and all other log records, including IP address captures, associated with the specified account; and
- f. Any records of communications between Microsoft/Skype, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider’s support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.